Blockchain Based Insurance System with KYC Verification

Ronan J. D'Souza[#1], Siddharth Dahiya[#2], Pranav V A[#3], Ishaan Dwivedi[#4], Jayakumar K.[*5]

[#]Student of School of Computer Science Engineering, Vellore Institute of Technology, Katpadi, Vellore, Tamil Nadu, India
[*]Associate Professor of School of Computer Science Engineering, Katpadi, Vellore, Tamil Nadu, India

---***---

Abstract - *The insurance industry has been in this world since the 1300's. While insurance is a high-hazard and exceptional yields industry, it additionally fills in as a shade for those out of luck. likewise ends up having total adaptability, as in, individuals are not qualified for stick to just a single arrangement. There are no restrictions on the quantity of policies which one can have. An implication of this is that they have to manage the surcharge for each policy, and also manage the consequences that originate with them. Extortion or fraud is a possible issue as the policyholder could exploit shortcomings in the case interaction (data unevenness and information storehouses). For the backup plan, it very well may be an expensive cycle due to manual organization, compromises, settling debates and so on for the policyholder, asserting the protection physically in the midst of hardship or pain is a disturbing circumstance. The particulars of the protection item are composed into a keen agreement which consequently pays out claims after getting the correct boundaries. This is plausible for basic "parametric" protection items where the case trigger occasion is effectively irrefutable from dependable openly accessible. Transactions are recorded on the blockchain for auditability to forestall different cases on a similar protected occasion. Utilizing blockchain likewise guarantees permanence and security. The data recorded to a blockchain is affix just, utilizing cryptographic strategies that assurance that once an exchange has been added to the record it can't be altered. This guarantees any modification. The system ensures security of data as everything is encrypted. The proposed system also eliminates the requirement of a middle man.*

Keywords— *blockchain, transactions, policyholder, cryptographic, encrypted*

1.INTRODUCTION

Since the early 1300's, the insurance industry has been in practice. It serves as an umbrella for those in need because of its high risk and high-returns industry. Since people are not entitled to stick to only one policy, therefore insurance also happens to have complete flexibility. There are even no maximum or minimum restrictions on the number of policies that a person can take. Since they have to manage the trouble that originate with the insurance, they have to even manage the premiums for every policy that they take because of the number restriction less policy. Coverage and security are all that matters when an unexpected disaster.

Many contribute to certain amount of fraudulent activities during the claim process, there by trying to take advantage of the existing system which considers being insured as important. Since a lot of people work with other basically a middleman, it usually leads to additional losses. What is highly undesirable is that documents and paper trails that lead to a plethora of confusion and unnecessary delays. There for now to achieve feasible and efficient solutions to the all the problems achieved is to make use of blockchain.

Making use of the extremely useful properties of blockchain will help to combat a lot of issues, especially the ones mentioned above. One of the most important property is immutability factor. If anyone tries to change their node, only their own is affects and this will prevent all the records from being changed. The next one is Smart Contracts. This is what will govern what data is added to the network and validates it as well. Since the blockchain network used is private and permissioned, it is developed using Hyperledger Fabric so that it will implement and gain the benefits of blockchain technology. Using this, tampering of data is resolved. Since everything is digitized, the need for a broker is eliminated. Unnecessary delay is ensured due to complete automation. Due to seamless access to old records, suspicious behaviour can be identified very easily and also this also eliminates double booking. Manual review is minimized because of transparency. Privacy is ensured because of how smart contracts govern how claims are added and also who is allowed to operate on them. Authenticity of a claim can be verified by the sources that are present on the same network.

Thus, using a blockchain system will effectively help combat these existing issues.

2. LITERATURE SURVEY

As indicated by the article on Forbes India, Managing characters of members is a bad dream for banks that are cling to follow the assignments. Endeavours to convey cross industry and between bank User Identification and check have fizzled as consistence can't acknowledge the legitimacy of information sourced from outside the bank, and each bank need to keep up various record.

This is trouble and moderate interaction, when a member in one bank needs to make exchange with other members in other bank. It is unimaginable except if the members are once more physically giving their personalities to other banks.

A straightforward and simple approach to arrangement is digitizing personality, be that as it may, this is a costly suggestion. As indicated by an industry report, banks and monetary foundations are spending more than $1billion on personality the board arrangements – without truly taking care of the issue as these are basic frameworks and advances which at times inconsistent.

3. DESIGN AND ARCHITECTURE

The Architecture of Blockchain is a kind of distributed data structure that keeps records about transactions and events. Blockchain can be seen as digitized ledgers which are replicated and distributed among the participants of the network.

The digital ledger sequentially records information about a transaction that is conducted. Each block is added to the previous block with the use of a cryptographic hash function resulting in a chain. The information stored in a blockchain is append-only, using encryption techniques that ensures that once a transaction has been added to the ledger it cannot be altered. This ensures inflexibility.

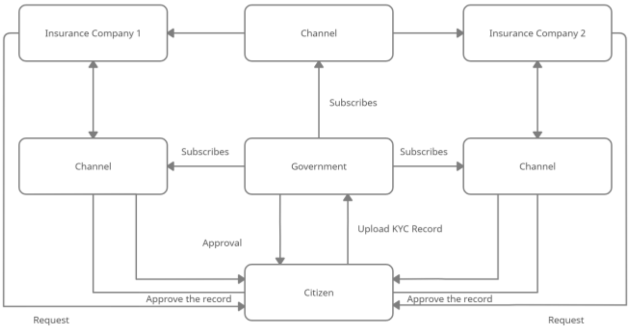


Figure 1 Architecture of system

3.1 Organizations

Organizations are the highest layer of a participating entity in the blockchain network. In our use-case, organizations will comprise the Central authority (Government agency), and the participating insurance companies.

These organizations consist of 1 or more peers that they own, and these peers are basically nodes participating in channels. Physically, peers signify individual “machines” or servers, that are a part of the main network.

3.2 Channels

Channels are virtually the “log” that a group of connected entities can view. For example, if we have 2 private firms A and B, 1 government firm and 1 citizen, we will ideally distribute the channels such that the dealings of the citizen with a private firm (A) are visible only to them and the government, and not the other private firm(B).

3.3 Orderers

Orderers are internal nodes that make sure the transactions committed in the distributed system are in the right order. These do not belong to any participating organization, and the blockchain administrators are responsible for maintaining it.

3.4 Certificate Authority

The Certificate Authority is the software tool responsible to maintain the identities and enrolments of the participating members.

3.5 Chaincode

Chaincode is the codified business logic of the network’s operation, the rules that define how and what data is stored, viewed, or modified.

These are all the nodes combined to form a bank organisation. Our application user identification and verification uses this architecture to solve the problem.

4. IMPLEMENTATION

Chaincode is a software program, coded in Go language, node.js, or in Java language that implements an interface. Chaincode runs in a Docker container which are secured and can be run on any OS platform separated from the endorsing peer process. Chaincode creates and manage those ledger state using participants applications transactions.

A chaincode normally oversees business rationale consented to by members of the organization, so it is same as the "smart contract", in open blockchain network. State made by a chaincode is made only to that chaincode and can't be gotten to straightforwardly by another chaincode. Notwithstanding, whenever given the proper authorization a chaincode may conjure another chaincode to access its state within the same network.

To implement the above solution, steps to be followed are: -

1) Import Hyperledger fabric docker from github to build the network

2) To create the network following steps are followed: -
(i.) Cloning of the Hyperledger fabric from the GitHub
(ii.) Doing changes in ‘DevServer_connection.json’ to create the required architecture for the network by defining all the entities for the designed system in JSON format.
(iii.) Master.sh scrip is need to execute to run and start the network.

(iv.) To access the system, use the keystore card of the organization to log in and enter into the system

3) When the network gets created, one organisation will receive 4 nodes called peer, Certificate Authority, Orderer, Couchdb.

4) After that the chaincode is deployed into each of the bank organisation.

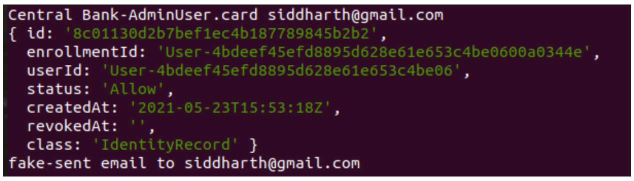
5) Now to access server one can use the APIs to call docekr containers.

The worker will utilize JSON Web Tokens for validation, an open norm (RFC 7519) that characterizes a smaller and independent path for safely sending data between parties as a JSON object. This data can be checked and trusted on the grounds that it is carefully marked. JWTs can be marked utilizing a mystery (with the HMAC calculation) or a public/private key pair utilizing RSA or ECDSA. Despite the fact that JWTs can be encoded to likewise give mystery between parties, we will zero in on marked tokens. Marked tokens can check the respectability of the cases contained inside it, while encoded tokens conceal those cases from different gatherings. At the point when tokens are marked utilizing public/private key combines, the mark likewise ensures that solitary the gathering holding the private key is the one that marked it.

The frontend will be integrated with the backend by making use of development packages included with NPM, and once the testing is complete, the frontend code will be transpired into pure JavaScript that can finally act as a monolithic web system.

5. RESULTS

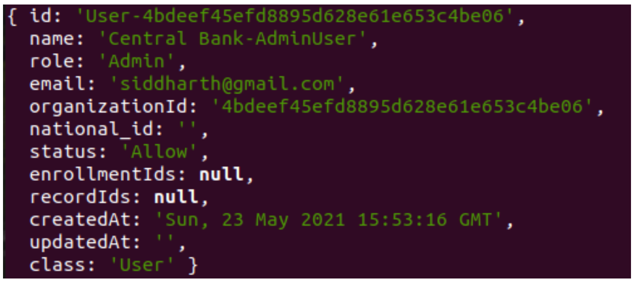
A screenshot of sample data which is fetch is placed below, that is between participants using API in JSON format:



```
Central Bank-AdminUser.card siddharth@gmail.com
{ id: '8c01130d2b7bef1ec4b187789845b2b2',
  enrollmentId: 'User-4bdeef45efd8895d628e61e653c4be0600a0344e',
  userId: 'User-4bdeef45efd8895d628e61e653c4be06',
  status: 'Allow',
  createdAt: '2021-05-23T15:53:18Z',
  revokedAt: '',
  class: 'IdentityRecord' }
fake-sent email to siddharth@gmail.com
```

Figure 2 Data to be fetched

Next is a screenshot of sample data fetched, which is between the banks.

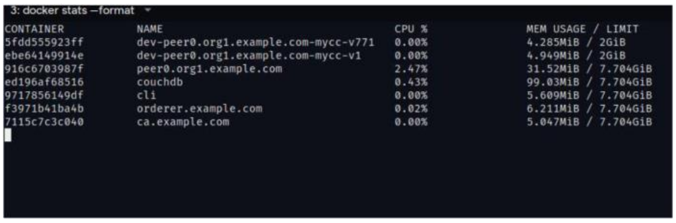


```
{ id: 'User-4bdeef45efd8895d628e61e653c4be06',
  name: 'Central Bank-AdminUser',
  role: 'Admin',
  email: 'siddharth@gmail.com',
  organizationId: '4bdeef45efd8895d628e61e653c4be06',
  national_id: '',
  status: 'Allow',
  enrollmentIds: null,
  recordIds: null,
  createdAt: 'Sun, 23 May 2021 15:53:16 GMT',
  updatedAt: '',
  class: 'User' }
```

Figure 3 Sample data fetched

Confidential information of a higher precedence is held by the bank only and never accessed by anyone including the participants which aren't inside the banks permissioned network. This makes it compile with all regulation of data privacy and protection.

The memory usage, performance and network impacts of the implemented system were measured. The entities in the network architecture are all in the form of docker containers, and are deployed to run as services.

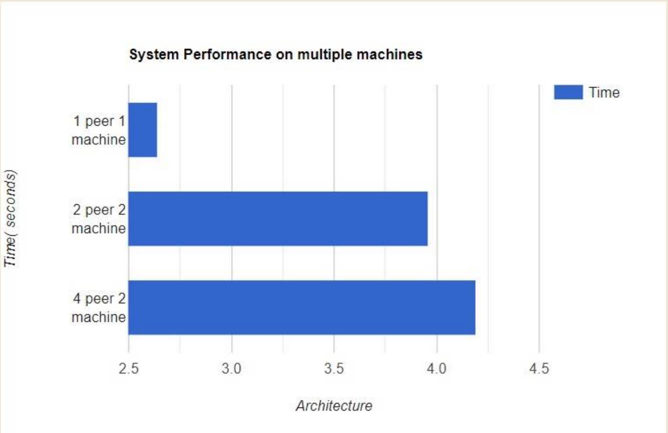


```
3: docker stats —format
CONTAINER      NAME                                  CPU %          MEM USAGE / LIMIT
5fdd555923ff   dev-peer0.org1.example.com-mycc-v771  0.00%          4.285MiB / 2GiB
ebe64149914e   dev-peer0.org1.example.com-mycc-v1    0.00%          4.949MiB / 2GiB
916c6703987f   peer0.org1.example.com                2.47%          31.52MiB / 7.704GiB
ed196af68516   couchdb                               0.43%          99.03MiB / 7.704GiB
9717856149df   cli                                   0.00%          5.609MiB / 7.704GiB
f3971b41ba4b   orderer.example.com                   0.02%          6.211MiB / 7.704GiB
7115c7c3c040   ca.example.com                        0.00%          5.047MiB / 7.704GiB
```

Figure 4 The entities in form of docker containers

The performance of the system based on multiple machines was measured, and these comprise two transaction types - commit transactions and data queries.

The result of the for commit transactions are tabulated and graphically represented below.



6. CONCLUSIONS AND FUTURE WORK

User identification and verification solution which are provided by blockchain to make the perfect platform so that it can deliver an automated, secure and trustworthy KYC. This also helps to improve participants experience, streamlines operational processes and enhances regulatory compliance.

Since the manual process of KYC is quite tedious, this can help to replace it. It can be developed further to form the general-purpose KYC solution that can also be done by making use of Blockchain Technology.

REFERENCES

[1] Gupta, Hima. "The role of insurance in health care management in India." International Journal of Health Care Quality Assurance 20.5 (2007): 379-391.

[2] Ellis, Randall P., Moneer Alam, and Indrani Gupta. "Health insurance in India: prognosis and prospectus." Economic and Political weekly (2000): 207-217.

[3] Bal, Meghna. "Securing property rights in India through distributed ledger technology." New Delhi: Observer Research Foundation (2017).

[4] Khatwani, Sudhir. “11 Blockchain Startups From India.” Coin Sutra: The Community of Cryptocurrency Lovers (2019)

[5] Boshuis, Susanne, et al. "The effect of generic strategies on software ecosystem health: the case of cryptocurrency ecosystems." Proceedings of the 1st International Workshop on Software Health. ACM, 2018.

[6] Higgins, S. Insurance Giant Allianz France Exploring Blockchain Potential. Available online: http://www.coindesk.com/allianz-franceexploring-use-cases-with-blockchain-startup/

[7] Insurance Times Newsdesk. AXA Leads $55m Investment in Blockchain. Available online: http://www.insurancetimes.co.uk/axaleads-55m-investment-inblockchain/1417270.article

[8] Lorenz, J.-T.; Münstermann, B.; Higginson, M.; Olesen, P.B.; Bohlken, N.; Ricciardi, V. Blockchain in Insurance-Opportunity or Threat? McKinsey & Company Report; McKinsey & Company: New York, NY, USA, 2016

[9] Shelkovnikov, A. Blockchain Applications in Insurance; Deloitte Report; Deloitte LLP: London, UK, 2016

[10] Maguire, Eamonn, et al. "Blockchain accelerates insurance transformation." KPMG Int (2017)

[11] McKinsey&Company. Blockchain Technology in the Insurance Sector. In Proceedings of the Quarterly Meeting of the Federal Advisory Committee on Insurance (FACI); McKinsey & Company: New York, NY, USA, 2017

[12] Higgins, S. European Insurance Firms Launch New Blockchain Consortium. Available online: http://www.coindesk.com/europeinsurance-blockchain-consortium/

[13] Klapkiv, Lyubov, and Jurij Klapkiv. "Technological innovations in the insurance industry." V1, Journal of Insurance, Financial Markets and Consumer Protection, 2017

[14] Gatteschi, Valentina, et al. "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?." Future Internet 10.2 (2018).